Electronic Communications Policy

Updated and Effective of: 4/1/2017

Responsible University Officer: Vice-President, Chief Information Officer (VP-CIO)

Policy Owner: Associate Vice-President, Information Technology

I. Purpose

The University recognizes the value and benefits that the use of electronic communications (EC) bring to the members of the University community (Users), enabling them to share information and ideas, collaborate, communicate, and conduct university business. EC includes the use of electronic mail (e-mail), calendar, text and voice messaging, and the University telephone system. These are collectively referred to as the ‘EC services’.

The University provides EC services to authorized users (e.g. faculty, staff and students) for the purpose of conducting University business. E-mail is an official means of communication at the University and authorized users are prohibited from using non-University e-mail accounts to conduct University business.

Users are required to follow normal acceptable standards of professional and personal ethics and conduct, and comply with the University’s Appropriate Use Policy when using the EC services. E-mail, text and voice messages should be managed appropriately in terms of their content whether sent or received.

Furthermore, e-mail accounts must not to be shared and each user is solely responsible for all actions performed under their account. Using and/or accessing EC services without proper authorization is prohibited. The University’s technical standards describe the approved e-mail system.

While the University takes reasonable measures to protect the privacy and confidentiality of EC services, and comply with applicable laws, regulations, and other University policies, the University does not guarantee this.

By implementing this policy the University will:

a. provide EC services to authorized Users who must use the provided services to conduct all University business,

b. ensure reasonable security policies, standards, controls, processes, practices, and procedures are in place to maintain the privacy, confidentiality, integrity and availability of the EC services,
c. restrict or deny access to the EC services as a result of policy violation, or unacceptable and inappropriate use,
d. in appropriate circumstances, reserve the right to inspect, review, monitor or disclose information such as e-mail, text and voice messages sent or received through its network, at its sole discretion when circumstances indicate such actions are necessary or required by law,
e. comply with all Federal, State, local laws and regulations, other University policies, and applicable agreements binding the University,
f. ensure this policy is consistently applied and monitored through the use of a compliance program.

II. Scope

This policy applies to all authorized Users who are provided with a University e-mail account (name@usfca.edu) and use the EC services either on- or off-campus.

III. Responsibilities

a. The Vice-President, Chief Information Officer (VP-CIO) designates the Associate Vice-President, Information Technology (AVP) to be responsible for the development and maintenance of this policy with consultation from the Office of the General Counsel (OGC).
b. The VP-CIO is responsible for approving and ensuring ongoing compliance with this policy with oversight from the Board of Trustees (BoT) Committee on Information Technology Strategy (CITS).
c. The University Leadership Team are responsible for championing this policy and information security practices in their respective Divisions, Schools, and Colleges, and any substantive revisions as recommended by the VP-CIO.
d. The VP-CIO is responsible for ensuring the EC services and associated information assets are secure from unauthorized access (to maintain appropriate confidentiality), unauthorized alterations (to maintain integrity), and available to authorized Users (to maintain availability) enabling the University to meet its mission in an effective and timely manner. The VP-CIO may delegate responsibility for this policy to the AVP.
e. The AVP is responsible for incorporating and maintaining reasonable security processes, practices, procedures, guidelines, and technologies to protect the EC services and assets, and ensure that this policy is reviewed and updated as necessary.
f. The Information Security Officer (ISO) is responsible for establishing and maintaining an information security program to support this policy and coordinate with the AVP on the ITS response to information security incidents, violations, or crimes committed under this policy. The Department of Public Safety is responsible for working with ITS, for conducting investigations, for preparing reports for the appropriate authorities, and providing support to authorities conducting their own investigations.
g. All Users, including Third-Parties entrusted with the University's information, are responsible for being familiar with, and complying with, this policy. Users have individual and shared responsibilities to protect the confidentiality, integrity, and availability of the EC assets in accordance with University policies, Federal, State, local laws, regulations, and
agreements binding the University. Users are required to take information security and awareness training appropriate to their role in support of this policy.

h. Users should understand that the University does not guarantee the privacy of information and should seek further guidance from the AVP if they are unsure of their responsibilities under this policy.

i. The OGC will provide legal guidance to this policy.

j. Failure to comply with this policy can result in actions to limit, suspend, or revoke user access to the University’s network, e-mail, and other information assets. Members of the University community who knowingly violate this policy may be subject to disciplinary actions that include but are not limited to the policies and procedures contained in the Staff Handbook, the Student Handbook (Fogcutter), applicable Collective Bargaining Agreements, and laws which may include civil and criminal prosecution.

IV. See Related Policies

a. Information Security Policy.

b. Technology Acquisition Life Cycle Management Policy.

c. Technology Resources Appropriate Use Policy.